AMENDMENTS TO THE SPECIFICATION

Pages 1-2, please replace paragraph [0006] with the following new paragraph:

[0006] The wireless data router ~~12~~ 14 assigns a temporary link layer address to the mobile station 10, and creates and initializes data structures used by wireless data protocols. A message containing the mobile's EID and the assigned link layer address is sent to the mobile station 10 by the wireless data router 14.

Page 2, please replace paragraph [0007] with the following new paragraph:

[0007] Wireless data networks encrypt transmissions over the airlink. Encryption key management is typically based on the Diffie-Hellman Electronic Key exchange procedure (e.g., Cellular Digital Packet Data networks use this procedure.) The Diffie-Hellman Electronic Key exchange procedure requires the network to generate a triplet (a, p, a^ymod p). The quantity a denotes an integer known to all mobiles using the network, p denotes a prime number known to all users using the network, and y denotes a secret random integer known only to the wireless data router 14. The wireless data router 14 sends this triplet to the mobile ~~system~~ station 10. The mobile station 10 performs its half of the Diffie-Hellman Electronic Key Exchange procedure by generating a secret random number x, and transmitting the quantity (a^xmod p) to the wireless data router 14. An encryption key is created by the mobile station 10 and the wireless data router 14 as the product (a^ymod p)(a^xmod p).

Page 2, please replace paragraph [0008] with the following new paragraph:

[0008] The mobile station 10 sends its network layer address (e.g., IP address) along with its "credentials," a shared secret known by only the network and the mobile station 10. The message containing this information is encrypted using the encryption key. The wireless data ~~network~~ router 14 sends a query to a authentication server 16. The authentication server 16 contains the current values of mobile station's credentials. The query contains the network layer address of the mobile station 10 as well as the credentials sent by the mobile station 10. The authentication server 16 checks the credentials against those stored in its database. If the credentials match, the authentication server 16 tells the wireless data router 14 to grant the mobile station 10 access to the network. New credentials may be generated and sent to the wireless data router 14 in the authentication response message. The wireless data router 14 informs the mobile station 10 of the result of its registration request. If the registration is successful the mobile station 10 is allowed access to the network. If new credentials were generated by the authentication server 16, the new credentials are also included in the registration response message.

Page 6, please replace paragraph [0023] with the following new paragraph:

[0023] If in step S16 the wireless data router 14 determines that the mobile station 10 is on the rogue mobile list, then in step S20 the wireless data router 14 increments the registration failure count for the mobile station 10 by one. Also, the wireless data router 14 determines if the incremented registration failure count equals or exceeds the registration failure threshold. If the threshold has not been reached, then processing

proceeds to step S14. However, if the threshold has been reached, then the wireless data router 14 sends a zap command to the mobile station 10 and then proceeds to step S14. The zap command instructs the mobile station 10 to disable its transmitter for a predetermined period of time called the leak delay. If the mobile station 10 obeys the zap command, then even the overhead associated with processing the link layer address request is avoided in addition to saving the airlink bandwidth.

Page 7, please replace paragraph [0025] with the following new paragraph:

[0025] As described, the database is automatically populated and depopulated requiring no manual intervention. When a mobile registration fails, that EID is placed into the database. More registration failures than the registration failure threshold ~~registration failures~~ during a period of time equal to the leak delay will result in the mobile being treated as a "true rogue", where link layer address requests will be ignored. The advantage here is that temporary network failures will not unfairly penalize a mobile station. It takes a persistent series of registration failures before the mobile station is tagged a "true rogue."